Department of Engineering and Architecture
University of Parma

Network Security
Exam 23/6/2020

1) What is a *chosen-plaintext* attack?

A. An attack scheme to a cryptographic system where the attacker can use several $\{m_i,c_i\}$ pairs, where m_i is the cleartext and $c_i=E_K(m_i)$ is the corresponding ciphertext
B. An attack scheme to a cryptographic system where the attacker can use several cleartexts $m_i=D_K(c_i)$, without knowing the key K neither the ciphertext c_i
C. An attack scheme to a cryptographic system where the attacker can choose some ciphertext messages c_i and, for each c_i, she can obtain the corresponding cleartext $m_i=D_K(c_i)$
D. An attack scheme to a cryptographic system where the attacker can choose some messages m_i and, for each m_i, he can obtain the corresponding ciphertext $c_i=E_K(m_i)$

2) What is the number of attempts required to perform a brute force attack against a secret key with *r* bits, used with a symmetric block cipher with block size *n* bits, supposing that you have some plaintext-ciphertext $\{m_i,c_i\}$ pairs?

A. n!
B. r*n
C. 2^n
D. 2^r

3) Diffie-Helmann is:

A. A symmetric block cipher algorithm
B. A symmetric stream cipher algorithm
C. An asymmetric block cipher algorithm
D. An asymmetric algorithm for key agreement/exchange

4) DSA is:

A. A symmetric block cipher algorithm
B. An asymmetric block cipher algorithm
C. A digital signature algorithm
D. A hash algorithm

5) Let us consider a One Time Password (OTP) authentication scheme that uses the Lamport's scheme, initialized with the user's secret *S*. If Alice wants to be authenticated by Bob, and if at the attempt number *t* Alice sends to Bob the value $H^n(S)$ as valid password, what is the next password sent at attempt number *t+1*? (Note: $H^n(S)$ indicates the execution of *n* times of the hash H on secret value *S*, i.e. $H^1(S)=H(S)$, $H^2(S)=H(H(S))$ ..)

A. $H^{2n}(S)$
B. $H^{n-1}(S)$
C. $H^{n+1}(S)$
D. $H^n(S+1)$

6) What do you need in order to verify the validity of a digital certificate?

A. the certificate of the CA that signed the given certificate
B. the private key of the CA that signed the given certificate
C. your own certificate

7) What is a CRL?

A. CA root List, that is the list of all root CAs
B. Certification Revocation List, that is a list issued by every CA that reports all certificates issued by the CA that are no more valid (revoked) while still not expired
C. Certification Root List, list of certificates that permits to back to the root CA, starting from a personal certificate

8) What is Euler's totient function?

8) What is Euler's totient function?

9) Given a symmetric block cipher $E_K()$, please show the first step and the generic *i*-step of the enciphering of a plaintext *m* using OFB (Output Feedback) mode. With $m=M_1||M_2||M_3|| .. ||M_i||M_{i+1}||..$

C0 = ?
Ci = ?

10) Suppose to use a block cipher with block size 4 bit. Using a given key *K* the $E_K()$ function encrypts input (plaintext) blocks according to the table on the right.

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000

Do encrypt the following plaintext *m* using OFP mode with IV=0001

m = 1100 0101 1100 0000

c= ?

11) Create a pair of RSA public/private key pair K^+=<e,n> (public) and K^-=<d,n> (private), starting from the two secret prime numbers p=5, q=11, and value *d*=23. For obtaining the value *e* of the public key, you can either use the Euclid's algorithm or try and test knowing that *d* is lesser than 20.
By using the public key K^+ do encrypt the plaintext *m*=4.

12) We want to store a large message *m* (e.g. a file) onto an insecure public storage system, by guaranteeing both the confidentiality and the integrity/authenticity of the data *m*. Let's suppose to have a private/public key pair K^- and K^+, and to have the following cryptographic algorithms: RSA, AES, SHA1. Please indicate a possible functional scheme that can be used for such a purpose, and the resulting data that will be actually stored.
(Note: if possible, use symmetric encryption for providing confidentiality)

13) Show an example of successful Man-in-the-middle attack against basic Diffie-Hellman exchange between two entities A and B.

14) An entity A has her private key K_A^-, her certificate $cert_{CA3}(A)$ (that is the certificate of A signed/issued by CA3), and the following additional certificates: $cert_{CA2}(CA3)$, $cert_{CA1}(CA2)$, $cert_{CA0}(CA1)$, and $cert_{CA0}(CA0)$.
An entity B has his private key K_B^-, his certificate $cert_{CA5}(B)$, and the following certificates: $cert_{CA4}(CA5)$, $cert_{CA1}(CA4)$, $cert_{CA0}(CA1)$, and $cert_{CA0}(CA0)$
Which is the minimum set of certificates that A must send to B in order to let B authenticate A using a challenge/response scheme based on public key cryptography (e.g. using the A's signature)?

15) The entity A wants to anonymously send a message *m* to B, by using a sequence of two high-latency anonymity nodes (Mix nodes) *P* and *Q*. Assuming that for each entity *X* (with *X*=*A*,*P*,*Q*,*B*), K^+_X and K^-_X are the public and private keys, what is the message that A sends to P?